REMARKS/ARGUMENTS

Claims 1-18 and 22-36 are currently pending. Claims 1, 28, 29, 32, 33, 34, and 36 have been amended and are supported by page 11, line 8, through page 13, line 5, Figure 2, and elsewhere in the original disclosure. It is respectfully submitted that no new matter has been added.

35 U.S.C. 103 Rejections

The Patent Office rejected claims 1-13, 15 and 17-34 under 35 U.S.C. 103(a) as being unpatentable over Kakemizu, U.S. Published Patent Application No. 2002/0018456, in view of Lee, U.S. Published Patent Application No. 2002/0085517, and Balaz, U.S. Published Patent Application No. 2006/0179298.

Claim 1 recites as follows:

> A network comprising: an internal secured portion comprising a first virtual private network certificate authority and a second virtual private network certificate authority; an external portion; at least one mobile node in the external portion; at least a first gateway associated with the first virtual private network certificate authority; and at least a second gateway associated with the second virtual private network certificate authority, where the internal secured portion connects via the first gateway and the second gateway to the external portion, and the network is configured to change a gateway, which the mobile node uses to communicate with the internal secured portion, from the first gateway to the second gateway via the first and the second virtual private network certificate authorities in response to movement of the mobile node and in response to a receipt from the mobile node of a new care-of-address that is different from a first care-of-address.

Independent claims 28, 33, and 34 recite subject matter similar to that recited by claim 1 such as "at least a first gateway associated with the first virtual private network certificate authority," "at least a second gateway associated with the second virtual private network certificate authority," and changing a gateway "from the first gateway to the second gateway via the first and the second virtual private network certificate authorities in response to movement of the mobile node."

Kakemizu discloses a virtual private network (VPN) that works in conjunction with a home authentication server. According to the second, third, fifth, and sixth exemplary embodiments (Figures 25, 26, 28, and 29 respectively) of Kakemizu a method to purportedly reconstruct a VPN when a mobile node moves is disclosed. In the second embodiment

beginning at paragraph [0113] and ending at paragraph [0117] of Kakemizu, the VPN is purportedly reconstructed after the user sends a registration request. This registration request includes the address of the old foreign agent. Paragraph [0113] of Kakemizu is reproduced below for reference purposes.

> In FIG. 25, when the MN 1 of the user has moved from the FA 21 to a new FA 21' within the same domain, a registration request message (Reg Req) that includes the address of the old FA 21 is transmitted as prescribed in the mobile IP path optimization draft (draft-ietf-mobileip-optim-09) ({circle over (1)}). The new FA 21' includes this registration request into an authentication request message (AMR) ({circle over (2)}), and transmits this authentication request message (AMR) to the local AAA server (AAAF) 23 within its own ISP 2. When the authentication request message (AMR) includes the old FA 21, the AAAF 23 extracts the VPN between the FA and the HA from the VPN information cache, and substitutes the address of the FA 21 with the address of the new FA 21'. Then, the AAAF 23 returns to the new FA 21' an authentication response message (AMA) that is added with a profile of the VPN to be set to the FA ({circle over (3)}).

As discussed in the last response, the address of the old foreign agent is not equivalent to a new care-of-address of the mobile node that is different from a first care-of-address.

Kakemizu does not teach or suggest "at least a first gateway associated with the first virtual private network certificate authority" and "at least a second gateway associated with the second virtual private network certificate authority" or changing a gateway "from the first gateway to the second gateway via the first and the second virtual private network certificate authorities in response to movement of the mobile node."

Lee discloses a handoff method in an IP telephony system where a gatekeeper supports handoff. Lee, in paragraph 0095, discloses as follows:

> when it is detected that MT2 has been moved to a different subnet of the same zone, that is, when it is detected that MT1 has been moved to a different subnet and becomes MT2, MT2 is assigned a care of address (COA: a new IP) by the foreign agent (FA) of the corresponding subnet and is requested to be registered for the gatekeeper (step S128). Upon receipt of a request of registration, the gatekeeper performs a handoff routine using the 3PPR signaling, since the terminal changes its IP during the call (step S129).

Lee, like Kakemizu, does not teach or suggest "at least a first gateway associated with the first virtual private network certificate authority" and "at least a second gateway associated with the second virtual private network certificate authority" or changing a gateway "from the first

gateway to the second gateway via the first and the second virtual private network certificate authorities in response to movement of the mobile node."

Balaz has been cited for teaching a virtual private network certificate authority.

Balaz discloses a virtual private network protocol gateway in which the protocol gateway is implemented as a registration authority that operates as an intermediary between routers and a certificate authority, allowing routers operating in accordance with one protocol to obtain and maintain certificates for a virtual private network from a certificate authority operating in accordance with another protocol.

Balaz discloses, e.g., in paragraphs 0007, 0036, 0046, and 0047, a single certificate authority.

Balaz, like Lee and Kakemizu, fails to disclose or suggest "at least a first gateway associated with the first virtual private network certificate authority" and "at least a second gateway associated with the second virtual private network certificate authority" or changing a gateway "from the first gateway to the second gateway via the first and the second virtual private network certificate authorities in response to movement of the mobile node."

Because each of these three references fail to disclose or suggest this claimed subject matter, any purported combination of these three references would fail to disclose or suggest this claimed subject matter.

Thus, claims 1-18, 22-28, 30, 31, and 33-35 are not made obvious by Kakemizu in view of Lee and Balaz.

Claim 29 recites as follows:

> A mobile node comprising: means for receiving, via a first secure communication means, an identifier of a second gateway; and means for changing from communicating with an internal secured portion of the network through the first gateway to communicating via the second gateway, in response to moving and sending a new care-of-address that is different from a first care-of-address to the first gateway, **wherein the mobile node enters a security association for the second gateway into its security association database**.

Claim 32 recites as follows:

> A method comprising: moving by a mobile node in an external portion of a network, where the network comprises an internal secured portion, the external portion, at least a first gateway, and at least a second gateway; obtaining a location identifier, where the location identifier comprises a

> new care-of-address different from a first care-of-address; sending the new care-of-address to the first gateway; and in response to receiving an acknowledgement from the second gateway, communicating via the second gateway, **wherein the mobile node enters a security association for the second gateway into its security association database.**

It is not seen where any of Kakemizu, Lee, or Balaz discloses the claimed subject matter of "**wherein the mobile node enters a security association for the second gateway into its security association database.**"

Thus, claims 29 and 32 are not made obvious by Kakemizu in view of Lee and Balaz.

The Patent Office rejected claims 14 and 16 under 35 U.S.C. 103(a) as being unpatentable over Kakemizu and Lee and Balaz, as applied to claims 1, 13, and 15 above, and further in view of Shapira, U.S. Patent No. 7,107,464.

Claims 14 and 16 have been rejected as obvious in regards to Kakemizu in view of Lee, Balaz, and Shapira. The Shapira reference fails to cure the shortcomings of Kakemizu, Lee, and Balaz. Claims 14 and 16 are both dependent on claims that should be allowed for reasons argued above, and therefore claims 14 and 16 should be allowed as well.

The Patent Office rejected claim 36 under 35 U.S.C. 103(a) as being unpatentable over Balaz, U.S. Published Patent Application No. 2006/0179298, in view of Kakemizu, U.S. Published Patent Application No. 2002/0018456.

Claim 36 recites as follows:

> A virtual private network certificate authority, comprising: means for forming first and second security associations between and with a mobile node and the virtual private network certificate authority; means for updating a location database; and means for forming first and second security associations between and with a gateway node and the virtual private network certificate authority, wherein the first and second security associations between and with the mobile node and the virtual private network certificate authority and between and with the gateway node and the virtual private network certificate authority are encapsulating security payload security associations.

The Patent Office asserted that paragraphs 0036 and 0037 of Balaz disclose "means for forming first and second security associations with a gateway node."

Paragraphs 0036 and 0037 of Balaz disclose as follows:

> [0036] In order for data to be transmitted among routers 110-114, a

> certificate-based authentication scheme is employed. In such an authentication scheme, each router 110-114 is assigned a unique certificate that it can use to authenticate itself to other routers or other computing devices (e.g., an ISP, a bridge or gateway, etc.). Additionally, these other computing devices may be part of VPN 106 and may similarly be assigned unique certificates that can be used for authentication. Such certificates can also optionally be used to encrypt messages between routers and/or other computing devices in any of a variety of conventional manners. For ease of explanation, routers are described as the devices that are obtaining and maintaining certificates for VPN 106. The establishment and operation of a VPN is well-known to those skilled in the art, and thus will not be discussed further except as it pertains to the invention.
> [0037] The certificates used by routers 110-114 are assigned by a trusted certificate authority (CA) 116. The process of obtaining such a certificate is referred to as "enrollment". In the illustrated example, routers 110-114 use a different enrollment protocol than is used by certificate authority 116. A registration authority 118 communicates with both routers 110-114 and certificate authority 116 and acts as an intermediary for enrollment, translating requests and responses in one protocol to another, as discussed in more detail below.

The Patent Office asserted that paragraphs 0080 and 0081 of Kakemizu disclose "forming first and second security associations with a gateway node." Claim 36 recites "means for forming first and second security associations between and with a gateway node and the virtual private network certificate authority."

Although Balaz discloses "The certificates used by routers 110-114 are assigned by a trusted certificate authority (CA) 116," Balaz does not disclose or suggest "means for forming first and second security associations between and with a gateway node and the virtual private network certificate authority."

Kakemizu does not remedy the above deficiency of Balaz.

Paragraphs 0080 and 0081 from Kakemizu disclose as follows:

> [0080] FIG. 13 shows an example of a processing flow of the VPN path determination control section 313. The VPN path determination control section 313 extracts the address of the VPNGW (FA) 21 at the MN 1 side from the request originating host address of the authentication request message (AMR) (S109). Further, the VPN path determination control section 313 searches the CN-GW address correspondence table 314 by the CN address read from the VPN database 34, and reads the address of the VPNGW 51 at the CN 52 side and the VPNGW type (S110).
> [0081] Next, when the VPNGW type is the one to which a VPN can be set dynamically, the process proceeds to step S112. When the VPNGW type is

> the one to which a VPN cannot be set dynamically, the process proceeds to step S113. In the present example, the processing at step S113 is carried out. The VPN path determination control section 313 sets the address of the HA 31 to the transmission originating GW address of the VPN information posted to the HA 31, and sets the address of the GW 51 read from the CN-GW address correspondence table 314 to the destination GW address. Further, the VPN path determination control section 313 sets the address of the FA 21 to the transmission originating GW address of the VPN information to be posted to the FA 21, and sets the address of the HA 31 to the destination GW address HA 31. Then, the VPN path determination control section 313 finishes the processing (sets a path to the FA, the HA and the CN).

There is no disclosure in paragraphs 0080 and 0081 of Kakemizu for the claimed subject matter of "means for forming first and second security associations between and with a mobile node and the virtual private network certificate authority."

Balaz does not remedy the above deficiency of Kakemizu.

Because neither Balaz nor Kakemizu disclose or suggest "means for forming first and second security associations between and with a mobile node and the virtual private network certificate authority" or "means for forming first and second security associations between and with a gateway node and the virtual private network certificate authority," any purported combination of Balaz and Kakemizu would fail to teach or suggest this claimed subject matter.

Furthermore, claim 36 recites "wherein the first and second security associations between and with the mobile node and the virtual private network certificate authority and between and with the gateway node and the virtual private network certificate authority are encapsulating security payload security associations." Although Kakemizu discloses encapsulated packets in, for example, paragraphs 0073, 0088-0091, and 0095, Kakemizu does not disclose "encapsulating security payload security associations." Balaz does not disclose "encapsulating security payload security associations" either. Because neither Kakemizu nor Balaz discloses "encapsulating security payload security associations," no purported combination of these two references would teach this claimed subject matter.

Thus, claim 36 is not made obvious by Balaz in view of Kakemizu.

The Patent Office is respectfully requested to reconsider and remove the rejections of the claims under 35 U.S.C. 103(a) and to allow all of the pending claims as now presented for examination. An early notification of the allowability of now pending claims 1-18 and 22-36 is earnestly solicited.

Respectfully submitted:

Walter J. Malinowski August 4, 2009

Walter J. Malinowski Date

Reg. No.: 43,423

Customer No.: 29683

HARRINGTON & SMITH, PC

4 Research Drive

Shelton, CT 06484-6212

Telephone: (203)925-9400, ext. 15

Facsimile: (203)944-0245

email: wmalinowski@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

8-4-09

Date Name of Person Making Deposit